TOWARDS AN AFRICAN VISION OF CYBERSECURITY GOVERNANCE

Koffi Fabrice DJOSSOU

The Global Forum 2016 - Eindhoven

Cybersecurity is “the prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and control systems.”*

African governance model for cybersecurity - Partnership for Critical Infrastructure Security and Resilience

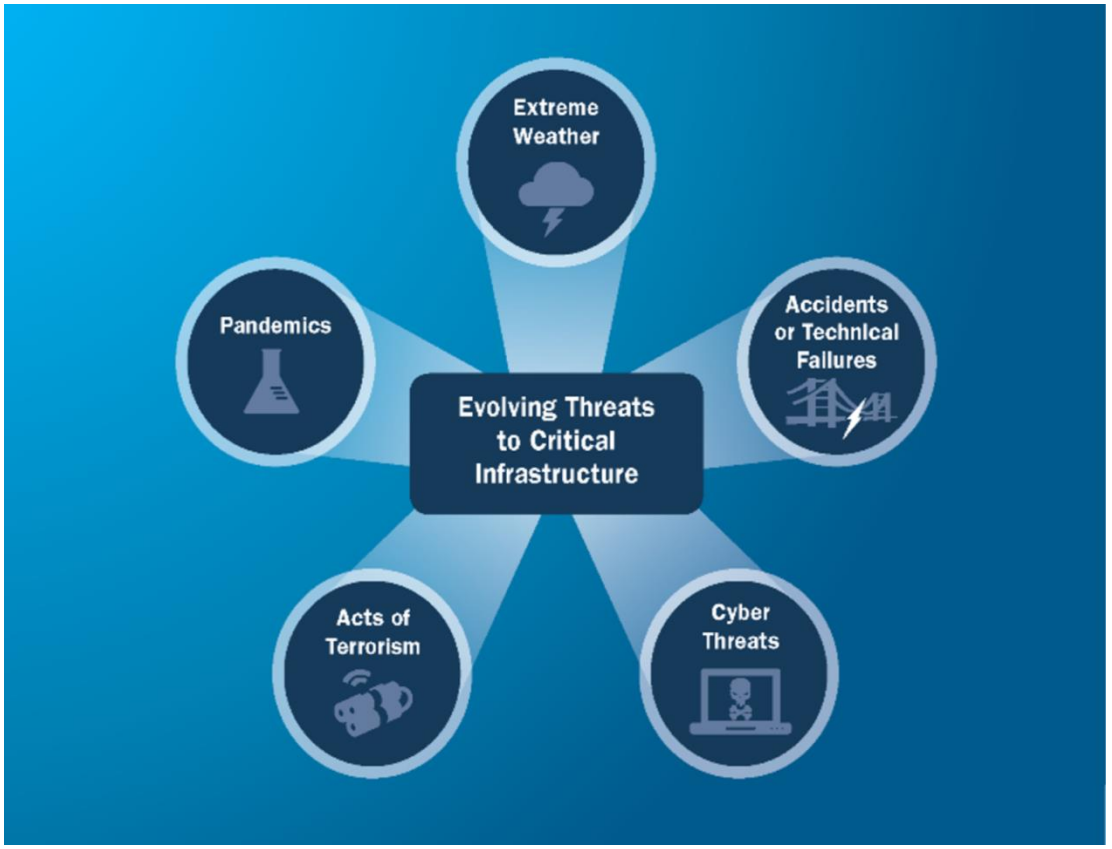
A continent in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened

Could it be an AFRICAN VISION

Today's Risk Landscape

The world at-large remain at risk from a variety of threats including:

- Acts of Terrorism
- Cyber Attacks
- Extreme Weather
- Pandemics
- Accidents or Technical Failures



Q: What could be the distributed approach for addressing the diverse and evolving risk environment.

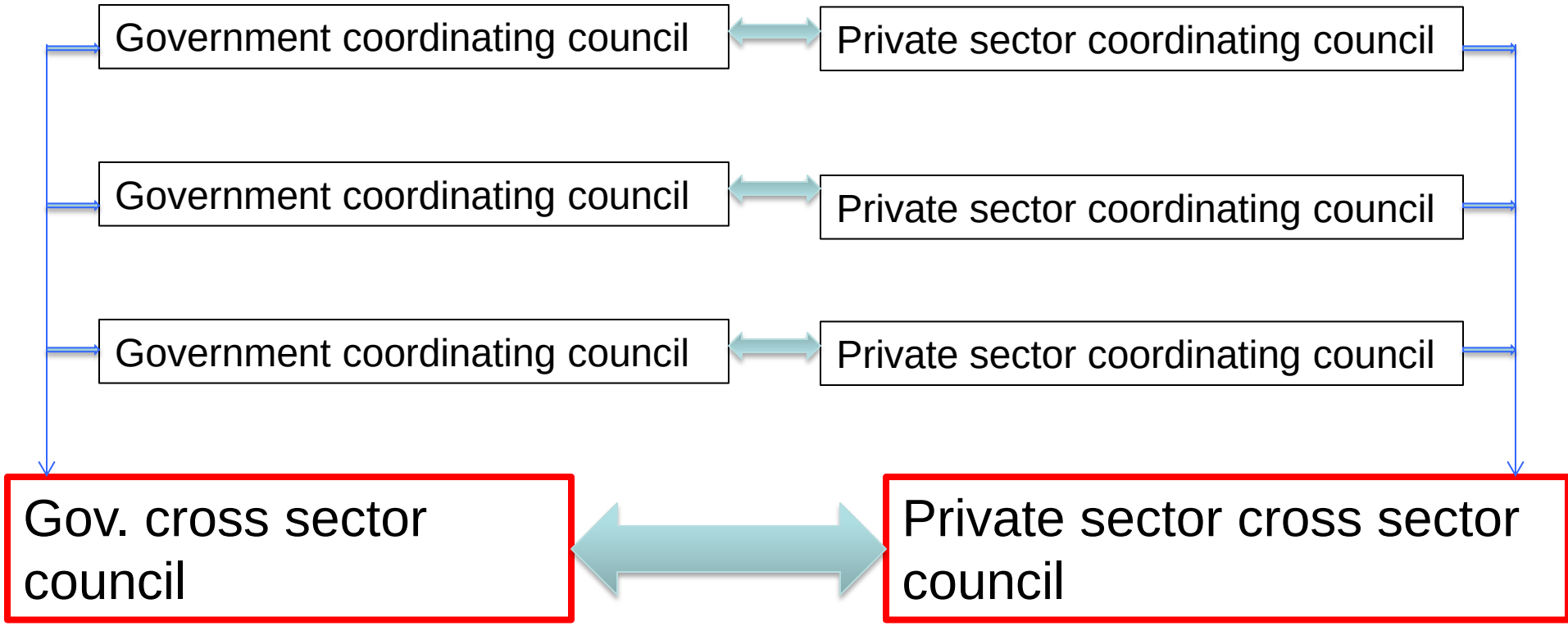
Critical Infrastructure Today

16 Critical Infrastructure Sectors

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Emergency Services
- Energy
- Financial Services
- Food & Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials and Waste
- Transportation Systems
- Water & Wastewater Systems

Public-Private Partnership

Public sector and private sector coordination



Strong Public-Private Partnership

Comparative Advantage

- Engaging in collaborative process
- Applying individual expertise
- Bringing resources to bear
- Building the collective effort
- Enhancing overall effectiveness

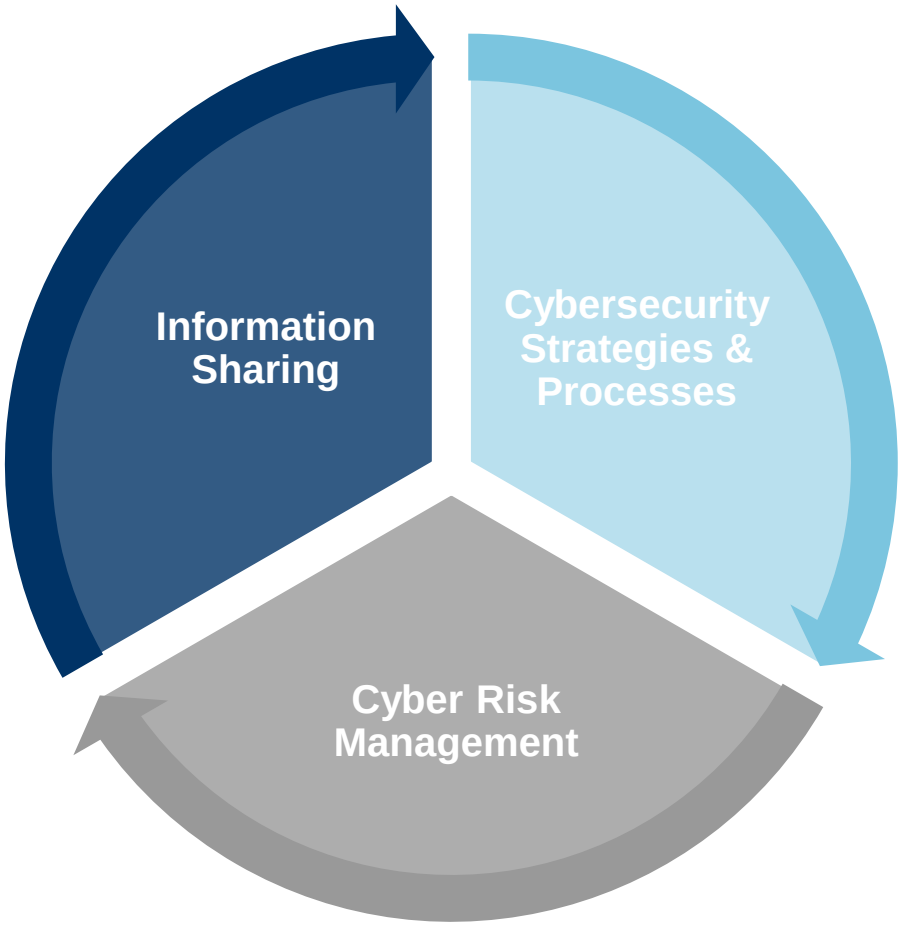
Private sector
- Customer relation
- Operation
- Investment

Country/National
- Law enforcement
- Public safety
- Regulation

African level
- National policy
- Information sharing
- Coordination

End-User
- Trusted relationship
- Community building
- Research

What should we do ?



Information-Sharing

- Provide sectors with cybersecurity and african governments information and establish bi-lateral expectations moving forward

Cybersecurity Strategies and Processes

- Share cybersecurity resources to help implement and manage cyber aspects through Risk Management Framework

Cyber Risk Management

- Assist sectors with implementing and managing cyber risk management activities

Protecting critical infrastructure through public-private partnerships

An african coalition through *partnerships* with the private sector, all levels of government, and international cooperation.

African public-private partnerships is key to strengthen cyber resilience

Towards an African Cybersecurity Agency

To facilitate government & industry partnerships to:

- Identify infrastructure and assess and prioritize risks
- Develop protective programs and measure program effectiveness.
- Identify, prioritize, and coordinate the protection of IT and critical communications infrastructure, including updating Sector-Specific Plans
- Setup and task a national team and focal
- Facilitate the public/government and private/industry working group meetings in coordination with the RECs
- Plan critical infrastructure protection (CIP) activities across various sectors and african countries
- Report on progress in the Critical Infrastructure National Annual Report

And an African Voluntary cybersecurity program : the research network

Cyber Resilience Review

Cybersecurity Education & Awareness Workforce Planning

Cyber Information Sharing and Collaboration Program

Enhanced Cybersecurity Services program

African Cybersecurity observatory

Q & A